HP MSM7xx Controllers Release Notes Version 6.5.0.0

Abstract

These release notes provide important release-related information for MSM software Version 6.5.0.0.

HP Part Number: 5998-6893
Published: November 2014
Edition: 1

Acknowledgments

Description

This document provides important V6.5.0.0 release information.

Products supported

This document applies to these HP products:

Product number	Model
J9693A	MSM720 Access Controller
J9694A	MSM720 Premium Mobility Controller
J9695A	MSM720 Access Controller (TAA)
J9696A	MSM720 Premium Mobility Controller (TAA)
J9421A	MSM760 Access Controller
J9420A	MSM760 Premium Mobility Controller
J9370A	MSM765 zl Premium Mobility Controller
J9840A	MSM775 zl Premium Controller

NOTE: Support for the discontinued MSM710 Controller is available in software versions prior to V6.2.x.

Upgrade information

Prerequisites

IMPORTANT: If your controller is not already running version 6.0.3.0 or later, a two-step upgrade must be performed. First upgrade your controller to Version 6.2.1.1, and then as a second step, upgrade the controller to V6.5.0.0. When V5.7.5.0 becomes available, you will be able to upgrade to it as the first step, prior to upgrading to V6.5.0.0.

Mandatory channel change required prior to software upgrade; discontinue use of channel 132

Applies to these Americas/USA models: MSM410 (J9426A/B), MSM422 (J9358A/B), MSM430 (J9650A), MSM460 (J9590A), MSM466 (J9621A), MSM466-R (J9715A), MSM310 (J9374A/B), MSM310-R (J9380A/B), MSM320 (J9360A/B), MSM320-R (J9365A/B), MSM325 (J9369A/B).

IMPORTANT: Prior to upgrading to MSM software Version 6.5.0.0, all applicable APs (autonomous or controlled) that are manually configured to use channel 132 must be either reconfigured to use a different channel or be reconfigured to use auto channel. This is required because channel 132 is no longer available for use.

NOTE: Due to a problem with AP channel use validation, a banner similar to this may appear at the top of the Home screen:

```
AP CNxxxxxxxx, Radio 1 channel configuration has been set to autochannel
because the previously configured channel is not supported by this version
of software.
```

The same message is added to the system log. These messages can be safely ignored.

Software configuration change may be required prior to upgrade

If the MSM7xx Controller is configured with the NAT feature enabled (default setting) and with the **Extend VSC egress subnet to VSC ingress subnet** feature enabled (disabled by default), the MSM software V6.5.x, V6.4.x, V6.3.x, or V6.2.x will disable the NAT feature. HP recommends that you review your existing settings and disable one of these features before upgrading to V6.5.x, V6.4.x, V6.3.x or V6.2.x.

Software Updates and Licensing portal

The Software Updates and Licensing portal provides access to the latest software updates to customers with a support contract. An HP Passport is required to access the Software Updates and Licensing portal at www.hp.com/go/hpsoftwareupdatesupport and it is available to customers who have purchased a maintenance and support agreement.

Upgrading restrictions and guidelines

Update the controller software as described in the "Software updates" section of the *MSM7xx Controllers Configuration Guide*. After the controller update is complete, it automatically updates all of its controlled devices to the same software version.

Transitioning APs from Unified controllers to use MSM software

Applies to these APs that have been used with any Unified controller (HP 10500/7500, HP 830, HP 850, HP 870, or HP WX5002/WX5004 Controller):

- HP 560
- HP 425
- MSM430
- MSM460
- MSM466
- MSM466-R

IMPORTANT: If any of these APs have ever been adopted by a Unified controller, it is mandatory to follow the procedures in the separate document *Instructions for Converting an Access Point from Unified-Controlled to Using MSM Software* before you can use these APs with MSM software (controlled or autonomous).

Downgrading software

If you upgrade to Version 6.5.0.0 and then want to return to the version that you had been running prior to upgrading, the configuration that you used originally with that version will still be available.

If you have made configuration changes while using Version 6.5.0.0, those changes will not be present when you downgrade to the previous version.

If you factory reset your device after upgrading to Version 6.5.0.0, your previous configurations will be lost, and when you downgrade to any previous version you will be in a factory reset state.

Compatibility/interoperability

MSM management tool

To run the management tool, use at least Internet Explorer 8 or Firefox 18.

NOTE: A web browser that supports SSLv3 is mandatory for running the MSM web-based management tool. SSLv3 is supported by Microsoft Internet Explorer 8 but it must be enabled. Microsoft Internet Explorer 9 and later use SSLv3 only. Mozilla Firefox also supports SSLv3 but support might need to be enabled or you might need to update to a more recent version.

RF Manager software and MSM software version compatibility

RF Manager Versions 6.0.x, and 6.7.x work with MSM software Version 5.7.x or later. However, to use the WLAN Integration feature in RF Manager 6.0.x or 6.7.x, the RF Manager and MSM software versions must be matched as follows:

MSM7xx software version	Compatible RF Manager versions	Sensor devices version	
		Sensor-only devices (MSM415)	AP/Sensor combo devices (MSM320[1], MSM325, HP 425[2])
6.3.0.0/6.4.0.0/6.4.1.0/6.5.0.0	6.7.769 or later	Upgraded automatically by RF Manager.	Upgraded automatically by MSM7xx Controller.
6.2.0.0	6.0.185, 6.7.769 or later		
5.7.1.x/5.7.2.0/6.0.0.1/6.0.1.x	6.0.177 or later		
5.7.0.2/5.7.0.3/5.7.0.4	6.0.162 or later		

[1] MSM320 APs that have been upgraded to MSM325 RF sensor via HP MSM320 RF Sensor License J9384A.

[2] HP 425 requires RF Manager V6.7.769.42 or later.

NOTE: Software Versions 6.2.0.0 and later are compatible with RF Manager versions listed above, but the MSM320 and MSM325 sensors may appear orange and indicate that there is a version mismatch. This is expected and the sensors will function normally. Note also, that with RF Manager 6.7.769, these sensors will function at an RF Manager 6.0.x feature level.

NOTE: If you choose to use mismatched software versions with RF Manager 6.0.177 or later, you should first turn off the WLAN Integration in RF Manager.

NOTE: Upgrading an MSM7xx Controller to V6.5.0.0 also automatically upgrades any MSM320 and MSM325 Sensors it manages to MSM software V6.5.0.0.

NOTE: The MSM415 Sensor has no MSM software dependency. It is managed and upgraded directly by RF Manager.

Local mesh

HP strongly recommends that for local mesh, the same AP model be used at both ends of the mesh link. If for local mesh, recent APs (MSM430, MSM46x, HP 425) are mixed with older APs (MSM3xx, MSM422), the local mesh connectivity might be unstable.

GMS (Guest Management Software)

HP GMS simplifies centralized guest-account creation from any Microsoft Windows-based computer. It provides centralized, real-time management of visitor accounts and sessions with a configurable visitor session duration per account. The intuitive user interface is designed for receptionists and clerical staff with minimal training. Working with HP MSM7xx Controllers, secure login prevents unauthorized account creation, and the reporting feature records all account management activity for audits. A digital certificate secures all communications between GMS and the MSM7xx Controller. For details and download instructions, consult the *Guest Management Software Release Notes*. Search for "Guest Management Software" at www.hp.com/support/manuals.

NOTE: GMS 6.5.0.0 works with and is required for MSM software Version 6.5.0.0 See also "GMS support for teaming" (page 6).

GMS support for teaming

GMS 6.5.0.0 supports teaming in MSM software 6.5.0.0 with the following limitations:

- **Only the team manager controller is supported.** GMS interacts only with the team manager controller and not member controllers.
- **Subscription plans not supported.** User sessions are not synchronized across all members in a team. Therefore, subscription plans are not supported on a controller team. User accounts cannot have **Validity** set to **Subscription Plan**. **Custom Validity** is the only choice for **Validity**.
- **Automatic account removal only supported for Invalidity.** Due to a lack of synchronization between team members and the team manager, automatic account removal due to **Inactivity** is not supported on a controller team. Automatic account removal due to **Invalidity** is supported on a controller team.
- **Maximum number of concurrent sessions not supported.** Since this option is per controller, it is not supported in a team. This option is fixed at **Unlimited** for controller teams.

Configuring the service controller in GMS (when teaming is used):

- Do not configure a controller in GMS when the team manager controller is not available and a team member is temporarily taking its place.
- GMS interacts only with the team manager controller, you cannot add a team member as the controller.
- Any attempt to add a team member as a service controller in GMS will be rejected, with the following message displayed: *"An error occurred while uploading the CA to the Service Controller. Please check if the Services Controller is a member of a team. If teamed, please add the Service Controller using the team IP or team manager IP."*
- It is best to use the team IP address for the controller configuration.
- If you specify the team manager controller IP address, GMS detects that it is the team manager controller and automatically adds the controller using the team IP address. This confirmation message is displayed: *"The Service Controller you are trying to add is the team manager. GMS will add this Service Controller using the team IP address instead of the Service Controller IP address."* This is normal.
- On the **Service Controller** tab, the **Edit Service Controller** button cannot be used to edit the controller information for teamed controllers (parameters such as Team IP, HTTP port number, and SOAP port number). Attempts to do this cause this message to be displayed: *"Editing Service Controller details is not supported. If the details are altered, please delete and add the Service Controller using the Add device wizard."* As the message indicates, delete and then add the controller back with the wizard, specifying the changed values.

Adding/editing user accounts in GMS when the team manager is unavailable:

- Like when teamed controllers are not used and the controller becomes unavailable, if the team manager controller becomes unavailable, users can still be added and edited in GMS but the controller (team manager) is not updated until it comes back online.
- In this case when adding/editing user accounts, the following prompt is displayed: `The selected team is in standby mode. GMS will add the account once the team manager is active. Do you want to continue?` Select **Yes** to add/edit the account in GMS only for now, with automatic update of the team manager controller upon its availability.

SOAP function limitations for teaming environment

The functions discussed in this section may be of interest to developers who make use of SOAP to communicate and configure devices, especially when creating and managing user accounts on a controller. The following SOAP function calls that were not available in previous versions are re-enabled in MSM software Version 6.2.0.0 or later.

- UpdateUserAccountMaxConcurrentSession: The user account limit is per controller instead of being applied globally to the team.
- UpdateUserAccountValidity: This function will return an error if subscription plans are selected to set the account validity.
- ExecuteUserAccountLogout: The action of logging out a user will only take effect if the user is logged in on the team manager.
- UpdateUserAccountRemovalSettings

The above limitations apply to controller teams only.

Although enabled in MSM software release 6.2.0.0 or later, the following SOAP functions should not be used on a controller team. If you attempt to use any of these functions when teaming is enabled, an error is returned.

- ExecuteBackupUserAccountsPersistentData
- ExecuteUserAccountRenewPlan
- AddSubscriptionPlan
- DeleteSubscriptionPlan
- DeleteAllSubscriptionPlans
- UpdateSubscriptionPlanName
- UpdateSubscriptionPlanOnlineTimeState
- UpdateSubscriptionPlanValidityPeriodState
- UpdateSubscriptionPlanOnlineTime
- UpdateSubscriptionPlanValidityPeriodMethodState
- UpdateSubscriptionPlanValidityPeriodFor
- UpdateSubscriptionPlanValidityPeriodBetween
- UpdateSubscriptionPlanValidityPeriodFrom
- UpdateSubscriptionPlanValidityPeriodUntil
- UpdateSubscriptionPlanBooleanAttribute
- UpdateSubscriptionPlanIntAttribute
- UpdateSubscriptionPlanBandwidthLevelAttribute

Note on SOAP function UpdateUserAccountRemovalSettings

The **Removal due to invalidity** option of this function works in a teaming environment. However, the **Removal due to inactivity** option should be avoided when teaming because it could cause the controllers to wrongly remove active accounts.

Enhancements

These new or changed features are included in this release:

New AP support

This release adds support for the HP 560 802.11ac Dual Radio Access Point.

802.11w support

This new VSC configuration option provides enhanced security for WPA2 traffic by protecting unicast and multicast management action frames. (HP 560 only.)

New installation configuration wizard

To help you perform the initial setup of the controller, a new configuration wizard is presented at startup. As a result, the **Configure initial controller settings** workflow has been removed from the **Automated workflows** feature.

RADIUS attributes for groups

(Applies to external RADIUS servers.) A new set of RADIUS attributes has been added allowing configuration of upload limits, download limits, and throughput rates for groups of users. Limits can be defined in terms of packets or octets (bytes). When a group quota is reached, the sessions for all users in the group are terminated.

Fixes

NOTE: The number that precedes the fix description is used for tracking purposes.

Version 6.5.0.0

These fixes are included in this release:

- [158413, 157094] Fixed an issue in which the management tool generated false errors when using the PayPal feature and HTML authentication.
- [152478, 157307] Applies when the addressing type (static/DHCP) of the egress interface is changed, or the IP address of the egress interface changes.) Fixed an issue in which DHCP relay functionality stopped working if an access controlled VSC is mapped to an egress interface that is associated with a VLAN on the Internet port, with NAT disabled, and the VSC's DHCP relay **Forward to egress interface** option is enabled.
- [151657, 157339] All wireless clients are now properly displayed on the Wireless clients page.
- [151413, 157319] (Applies to use of external DHCP servers.) Fixed an issue in which upon IP address renewal, wireless clients lost network connectivity, even though they remained associated with the AP.
- [151254, 158508] Wireless client authentication no longer stops functioning under the following circumstances:
  - There is one VSC configured for Active Directory authentication and one VSC configured for local authentication
  - A client authenticates on the VSC with Active Directory
  - Clients try authenticating on the VSC with local authentication
- [150082, 154710] Fixed an issue in which the filtering function on the Wireless Clients page did not work properly due to abbreviated AP names or SSIDs adversely affecting the filtering.

- [149941, 157372] (Applies to teaming.) AP group names longer than 20 characters, no longer cause temporary brief communication interruptions between teamed controllers.
- [149260, 157633] Fix to support Class attribute in Accounting request to external Radius servers when using non-access-controlled VSCs.
- [148577, 154038] (Applies to MSM775) Fixed an issue in which the LAN port occasionally operated with poor performance or failed to come up.
- [148398] Synchronizing AP configuration changes are no longer affected if any **Allowed wireless rates** check boxes are cleared.
- [147657] If system-wide Auto-channel/Auto-power is enabled, it is now possible to configure the Auto-channel and Auto-power Interval for an AP radio participating in local mesh.
- [146207, 157325] Fixed an issue in which after some period of time a recurring log message appeared, similar to:

  ```
  Jan 15 12:46:36 10.214.8.157 MSM775 debug statspoller: Process jpatch
  died with return code 11
  ```

  Network bandwidth was reduced, with the impact becoming more severe with a greater number of APs being adopted by the controller.
- [144311, 157477] Fixed an issue that occurred when a wireless client disassociated and then reassociated after a interval of more than 5 minutes, and the bandwidth restrictions imposed by the user account did not take effect.
- [142469] When using option **Public IP addresses for Guest Access**, if there are more wireless clients than available public IP addresses, the wireless clients with a public IP address already assigned do not lose their address to a new wireless client.
- [141161, 157631] (Applies to MSM310, MSM320, MSM422.) Unsupported channels 184,188,192 and 196 are no longer available on APs operating in Japan.
- [140584] The "**%**" character no longer causes random characters to appear in the name on the controller when used in creating a profile name. You can now use the "**%**" character when creating a profile name.

Issues and workarounds

NOTE: The number that precedes the issue description is used for tracking purposes.

The following issues are present in this release:

- [159677] The management tool may restart when attempting to sort a list of user sessions by VSC, Idle time or VLAN, when the list includes non-Access Controlled clients. You must log in again.
- [159082] Some clients might not be able to connect to a particular wireless network if the VSC has both **Protected Management Frames (802.11w)** and **Terminate WPA at the Controller** enabled. These are mutually exclusive options, even though the V6.5.0.0 software does not enforce mutual exclusivity.
- [158228] (Applies to teaming.) If an SNMPv3 user is configured in an SNMP Trap receiver on the team member controller, and the SNMPv3 user account is then deleted from the team manager controller, after a software upgrade, the team member controller can get stuck in a loop resetting and downloading a configuration. As a workaround, ensure that the team manager and team member controllers are synchronized before performing any software upgrade.
- [157935] An MSM7xx Controller will not communicate with an IMC server when the IMC server is identified with a fully-qualified domain name (FQDN). As a workaround, identify the IMC server by its IP address.

- [157512] If a network that has DHCP servers on multiple VLANs experiences DHCP server delays or interruptions, APs may allow clients to associate without getting an IP address. You can consider provisioning a specific discovery VLAN to help prevent this.
- [156141] An HP 560 can take several minutes to synchronize with a controller when creating or deleting a VSC with **Protected Management Frames (802.11w)** enabled.
- [156126] APs will not synchronize with a controller when all but the lowest data rates are disabled in a VSC.
- [154246] (Applies when (prior to upgrading to V6.5.0.0) under **Management** > **Device Discovery**, the **Mobility controller discovery** option is enabled and the address is specified in **IP address of the primary mobility controller**.) After upgrading to V6.5.0.0, the **Mobility controller discovery** option is disabled (although the IP address value is still retained). To correct this, re-enable the **Mobility controller discovery** option, and then select **Save**.
- [154123] If 16 VSCs are configured, it can take up to five minutes for an HP 560 to synchronize with a controller.
- [153856] (Applies to HP 425 with Country set to Taiwan.) If you configure channel 144 at the group level and adopt an HP 425 into that group, the HP 425 will not synchronize with the controller. The HP 425 does not have regulatory certification to operate using channel 144 in Taiwan, even though channel 144 can now be used there. As a workaround, adopt the HP 425 into a group that does not include channel 144 in its radio configuration.
- [152434] If your controller is not already running version 6.0.3.0 or later, a two-step upgrade must be performed. First upgrade your controller to Version 6.2.1.1, and then as a second step, upgrade the controller to V6.5.0.0. When V5.7.5.0 becomes available, you will be able to upgrade to it as the first step, prior to upgrading to V6.5.0.0.
- [149596] (Applies to teaming.) If the team manager fails, the interim team manager will enable RRM severe interference mitigation and AP load balancing, even if these options were disabled by the administrator. As a workaround, promote the interim team manager to team manager, and then disable undesired options.
- [148443] On the **Overview** > **Wireless clients** page, the scroll bar might be missing (or partially hidden) when viewed with Mozilla Firefox. The page displays properly when viewed with Microsoft Internet Explorer.
- [148260] (Applies to MSM720.) A timeout can occur when attempting to obtain the Sysinfo file from an MSM720 team manager when the team manager is under heavy load.
- [140224] (Applies to MSM410, HP 425, MSM430, MSM460, MSM466, MSM466-R.) When **Intrusion Detection System** (IDS) is enabled, AP radios on that (team of) controller(s) should not be configured in **Access Point and Local Mesh** or **Local Mesh only**. As a workaround, IDS must be disabled on the controller if **Access Point and Local Mesh** or **Local Mesh only** operation is required.
- [137197] When IMC establishes a connection to the MSM7xx Controller, the following error messages are displayed on the system log:

  ```
  err pmmclient: setVLANSubsectionIndexFromVLANNetworkProfileName: Unknown vlan name 'Internet port network'.
  ```

  ```
  err pmmclient: setVLANSubsectionIndexFromVLANNetworkProfileName: Unknown vlan name 'LAN port network'.
  ```

  ```
  err pmmclient: DB: Unable to prepare the SQL statement.
  ```

  ```
  err pmmclient: Could not get data from the database.
  ```

  These messages can be safely ignored.
- [131693] iPads/iPods/iPhones cannot authenticate using the secondary RADIUS server with the default configuration. As a workaround, reduce the retry interval in the RADIUS Profile configuration to 5 seconds.

- [131182] Re-deploying an AP from one controller to another controller might generate false attacks reported by IDS on the original controller. As a workaround, reboot the controller after removing the AP.
- [129915] Clients using the PPTP VPN server might experience connectivity issues when sending large packets.
- [127299] The SNMP OIDs that report information about the configuration of the Autochannel features “COLUBRIS-DEVICE-WIRELESS-MIB coDevWirIfStaAutoChannelEnabled” and “coDevWirIfStaAutoChannelInterval” may report incorrect information on the MSM410, MSM430, MSM460, MSM466, and MSM466-R.
- [124010] (Applies to MSM410, MSM430, MSM460, MSM466, MSM466-R in autonomous mode.) The Neighborhood Scanning feature configured to scan on all channels only scans on channels within the regulatory domain's approved channel list rather than all channels in the respective band. For example, with the location set to the United States, Neighborhood Scanning will not scan channels 12 or 13 since they are not part of the U.S. regulatory domain. This is true in both the 2.4 GHz and 5 GHz bands. There is no workaround.

Documentation updates and corrections

Online help

- Although referenced in the online help, the MSM710 Controller and MSM335 AP are not supported in release 6.5.0.x.
- The Protect Management Frames (802.11w) section in the online help contains the following statement:

  ```
  Only disable this option if you are having connectivity issues with 802.11w client stations, and
  disabling this option resolves the issues. Otherwise, this option should always be enabled.
  ```

  Ignore this help text, referring to the following text instead:

  To avoid compatibility issues with incorrect 802.11w implementations, the Protect Management Frames feature is disabled by default. It should only be enabled if your client stations provide a proper 802.11w implementation. One way to test this is to enable 802.11w support, and then see if wireless throughput decreases for a client station. If it does, the 802.11w implementation on the client is incompatible, and Protected Management Frame feature should not be enabled.

HP MSM SNMP MIB Reference Guide v6.5.0.x

The following objects in the COLUBRIS-VIRTUAL-AP-MIB are obsolete:

- coVirtualApAuthenMode
- coVirtualApAuthenProfileIndex
- coVirtualApUserAccountingEnabled
- coVirtualApUserAccountingProfileIndex
- coVirtualApDefaultUserRateLimitationEnabled
- coVirtualApDefaultUserMaxTransmitRate
- coVirtualApDefaultUserMaxReceiveRate
- coVirtualApDefaultUserBandwidthLevel

Contacting HP

For additional information or assistance, contact HP Networking Support:

http://www.hp.com/networking/support

Before contacting HP, collect the following information:

- Product model names and numbers
- Technical support registration number (if applicable)
- Product serial numbers
- Error messages
- Operating system type and revision level
- Detailed questions

HP security policy

A Security Bulletin is the first published notification of security vulnerabilities and is the only communication vehicle for security vulnerabilities.

- Fixes for security vulnerabilities are not documented in manuals, release notes, or other forms of product documentation.
- A Security Bulletin is released when all vulnerable products still in support life have publicly available images that contain the fix for the security vulnerability.

To find security bulletins:

1. Go to the HP Support Center website at www.hp.com/go/hpsc.
2. Enter your product name or number and click **Go**.
3. Select your product from the list of results.
4. Click the **Top issues & solutions** tab.
5. Click the **Advisories, bulletins & notices** link.

To initiate a subscription to receive future HP Security Bulletin alerts via email, sign up at:

http://h41183.www4.hp.com/signup_alerts.php?jumpid=hpsc_secbulletins

Related information

Documents

To find related documents, see the HP Support Center website:

http://www.hp.com/support/manuals

Enter your product name or number and click **Go**. If necessary, select your product from the resulting list.

See also the "New in release" section of the *MSM7xx Controllers Configuration Guide*.

Websites

- Official HP Home page: http://www.hp.com
- HP Networking: http://www.hp.com/go/networking
- HP product manuals: http://www.hp.com/support/manuals
- HP download drivers and software: http://www.hp.com/support/downloads
- HP software depot: http://www.software.hp.com
- HP education services: http://www.hp.com/learn

Documentation feedback

HP is committed to providing documentation that meets your needs. To help us improve the documentation, send any errors, suggestions, or comments to Documentation Feedback

(docsfeedback@hp.com). Include the document title and part number, version number, or the URL when submitting your feedback.